We Claim:

1. A method for use in a system which includes a cryptographic key store for storing a transformed cryptographic key and accessing circuitry for accessing the transformed cryptographic key from the cryptographic key store, the method comprising the step of:

storing key re-transforming information for the transformed cryptographic key in a decryption store, the accessing circuitry being able to communicate with the decryption store exclusively via a predetermined interface, the interface being such that the accessing circuitry is unable to access from the decryption store at least one of: a) at least a portion of the key re-transforming information, and b) at least a portion of the cryptographic key.

2. The method of claim 1 wherein the interface is such that the accessing circuitry is unable to access from the decryption store both of: a) at least a portion of the key re-transforming information, and b) at least a portion of the cryptographic key.

3. The method of claim 1 wherein the key re-transforming information comprises:

a transformation pattern; and

a key decrypting algorithm.

4. The method of claim 3 wherein the transformation pattern comprises a unique identifier of the decryption store.

5. The method of claim 1 further comprising the steps of:

the decryption store receiving the cryptographic key;

the decryption store transforming the cryptographic key using key transforming information to produce the transformed cryptographic key; and

the decryption store sending the transformed cryptographic key to the cryptographic key store.

6. The method of claim 1 wherein:

the decryption store comprises a mobile terminal;

the cryptographic key store comprises a computer memory; and

the accessing circuitry comprises a processor.

7. The method of claim 1 wherein:

the decryption store comprises a network access card;

the cryptographic key store comprises a computer memory; and

the accessing circuitry comprises a processor.

8. The method of claim 1 further comprising the steps of:

the decryption store receiving the transformed cryptographic key and information;

the decryption store re-transforming the transformed cryptographic key using the key re-transforming information to produce the cryptographic key; and

the decryption store encrypting the information using the cryptographic key to produce encrypted information.

9. The method of claim 8 further comprising the step of transmitting the encrypted information.

10. The method of claim 1 further comprising the steps of:

the decryption store receiving encrypted information;

the decryption store receiving the transformed cryptographic key;

the decryption store re-transforming the transformed cryptographic key using key re-transforming information to produce the cryptographic key; and

the decryption store decrypting the encrypted information using the cryptographic key to produce decrypted information.

11. The method of claim 10 further comprising the step of the accessing circuitry accessing the decrypted information.

12. The method of claim 1 wherein the accessing circuitry's communication with the decryption store comprises the transfer of information between them.

13. The method of claim 1 wherein the storing step comprises storing the transformed cryptographic key in the cryptographic key store for a period of time.

14. The method of claim 1 further comprising the step of erasing the cryptographic key from the decryption store at the completion of each cryptographic operation.

15. The method of claim 1 wherein the cryptographic key is stored in the decryption store in such a way that it disappears from the decryption store when the decryption store is removed from the system.

16. A system comprising:

a cryptographic key store for storing a transformed cryptographic key;

a decryption store for storing key re-transforming information for the transformed cryptographic key, the decryption store having a predetermined interface;

accessing circuitry coupled to the cryptographic key store, the accessing circuitry being able to access the transformed cryptographic key in the cryptographic key store, and to communicate with the decryption store exclusively via the predetermined interface, the interface being such that the accessing circuitry is unable to access from the decryption store at least one of: a) at least a portion of the key re-transforming information, and b) at least a portion of the cryptographic key.

17. The method of claim 16 wherein interface is such that the accessing circuitry is unable to access from the decryption store both of: a) at least a portion of the key re-transforming information, and b) at least a portion of the cryptographic key.

18. The system of claim 16 wherein:

the decryption store comprises a mobile terminal;

the cryptographic key store comprises a computer memory; and

the accessing circuitry comprises a processor.

19. The system of claim 16 wherein:

the decryption store comprises a network access card;

the cryptographic key store comprises a computer memory; and

the accessing circuitry comprises a processor.

20. The system of claim 16 wherein the decryption store further comprises:

an input port for receiving the transformed cryptographic key;

a key decrypting module for decrypting the transformed cryptographic key using the key re-transforming information to produce the cryptographic key;

an encrypting module for encrypting information using the cryptographic key to produce encrypted information.

21. The system of claim 20 wherein the decryption store further comprises a transmitter for transmitting the encrypted information.

22. The system of claim 16 wherein the decryption store further comprises:

an input port for receiving the transformed cryptographic key;

a key decrypting module for decrypting the transformed cryptographic key using the key re-transforming information to produce the cryptographic key;

a decrypting module for decrypting encrypted information.

23. The system of claim 22 wherein the decryption store further comprises a receiver for receiving the encrypted information.

24. The system of claim 16 wherein the decryption store further comprises:

a receiver for receiving the cryptographic key;

a key encrypting module for encrypting the cryptographic key using key transforming information to produce the transformed cryptographic key; and

an output port for outputting the transformed cryptographic key.

25. A decryption store for storing key re-transforming information for a transformed cryptographic key, the decryption store comprising:

a predetermined interface, the interface being operable to receive the transformed cryptographic key; and

an output port complying exclusively with the predetermined interface such that information is accessible from the decryption store through the output port;

wherein at least one of: a) at least a portion of the key re-transforming information, and b) at least a portion of the cryptographic key being not accessible from the decryption store through the output port.

26. The method of claim 25 wherein interface is such that at least both of: a) at least a portion of the key re-transforming information, and b) at least a portion of the cryptographic key are not accessible from the decryption store through the output port.

27. The invention of claim 25 wherein the decryption store comprises a mobile terminal.

28. The invention of claim 25 wherein the decryption store comprises a network access card.

29. The invention of claim 25 wherein the decryption store further comprises:

a key decrypting module for decrypting the transformed cryptographic key using the key re-transforming information to produce the cryptographic key;

an encrypting module for encrypting information using the cryptographic key to produce encrypted information; and

a decrypting module for decrypting encrypted information.

30. The invention of claim 29 wherein the decryption store further comprises a transmitter for transmitting the encrypted information.

31. The invention of claim 25 wherein the decryption store further comprises:

a receiver for receiving the cryptographic key;

a key encrypting module for encrypting the cryptographic key using key transforming information to produce the transformed cryptographic key.

32. The invention of claim 31 wherein the transformed cryptographic key is a function of a transformation pattern.

33. The method of claim 32 wherein the transformation pattern comprises a unique identifier of the decryption store.

34. A method for use in a decryption store having a predetermined interface and an output port complying exclusively with the interface such that information is accessible from the decryption store through the output port and at least one of: a) at least a portion of the key re-

transforming information, and b) at least a portion of the cryptographic key, is not accessible from the decryption store through the output port, the method comprising the step of:

storing key re-transforming information for a transformed cryptographic key in the decryption store;

receiving the transformed cryptographic key; and

decrypting the transformed cryptographic key to produce the cryptographic key.

35. The method of claim 34 wherein the interface is such that at least both of: a) at least a portion of the key re-transforming information, and b) at least a portion of the cryptographic key are not accessible from the decryption store through the output port.

36. The method of claim 34 wherein the key re-transforming information comprises:

a transformation pattern; and

a key decrypting algorithm.

37. The method of claim 36 wherein the transformation pattern comprises a unique identifier of the decryption store.

38. The method of claim 34 further comprising the steps of:

the decryption store receiving the cryptographic key;

the decryption store transforming the cryptographic key using key transforming information to produce the transformed cryptographic key; and

the decryption store sending the transformed cryptographic key to a cryptographic key store via the output port.

39. The method of claim 34 wherein the decryption store comprises a mobile terminal.

40. The method of claim 34 wherein the decryption store comprises a network access card.

41. The method of claim 34 further comprising the steps of:

the decryption store receiving information; and

the decryption store encrypting the information using the cryptographic key to produce encrypted information.

42. The method of claim 41 further comprising the step of transmitting the encrypted information.

43. The method of claim 34 further comprising the steps of:

the decryption store receiving encrypted information; and

the decryption store decrypting the information using the cryptographic key to produce decrypted information.

44. The method of claim 43 further comprising the step of sending the decrypted information to accessing circuitry via the output port.